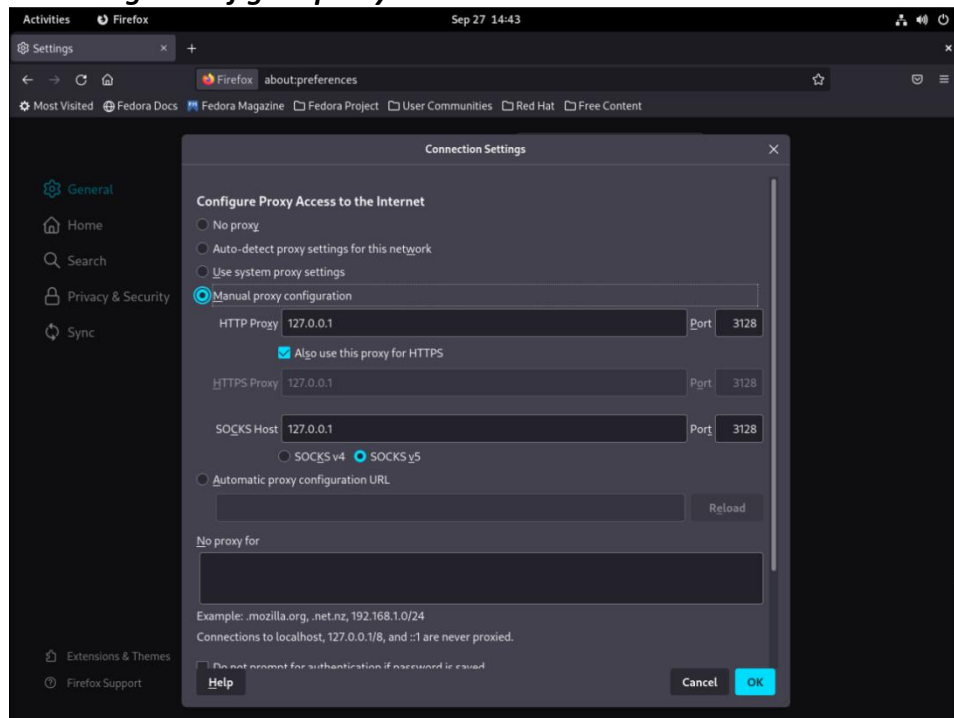


SQUID (Non Transparent)

Roll No: 1942

1. Install squid (if required).
dnf install squid
2. How to start/restart/stop squid service.
systemctl status/start/stop/restart squid
3. Change browser proxy setting to use squid proxy.
Mozilla firefox -> setting -> configure proxy



4. squid configuration file is located in /etc/squid. Any modifications to squid configuration file needs squid service restart.
5. Keep a copy of squid configuration file.
cat /etc/squid/squid.conf > /etc/squid/squid.conf.backup
6. List of assignments to complete (configuration file to be restored to original before starting with each assignment.) – Non Transparent Proxy mode.
 1. Check that all websites (http and https) are accessible.
(default squid.conf)
 2. Block Amazon and Flipkart.
acl blacklist dstdomain www.amazon.com
acl blacklist dstdomain www.flipkart.com

http_access deny blacklist

http_access allow all
 3. Block all websites except Amazon and Flipkart.
acl blacklist dstdomain www.amazon.com
acl blacklist dstdomain www.flipkart.com

http_access allow blacklist

http_access deny all

4. Block all websites between 9 am to 5 pm. (Since the lab is scheduled between 2 to 5 pm , all websites should be blocked).

acl mcaTime time 9:00-17:00

http_access deny mcaTime

http_access allow all

5. Change block timing to 9 am to 1 pm. (All websites should be accessible now).

acl mcaTime time 9:00-13:00

http_access deny mcaTime

http_access allow all

6. Block access to Amazon and Flipkart between 2 to 5 pm. Allow all other sites.

acl blacklist dstdomain www.amazon.com

acl blacklist dstdomain www.flipkart.com

acl blockShopTiming time 9:00-13:00

http_access deny blockShopTiming blacklist

http_access allow all

7. Create three users, Alice, Bob, Darth.

-c (for new file)

-m (for MD5 algorithm, if not specified default is MD5)

```
[root@fedora nehalparsekar]# htpasswd -c -m /etc/squid/passwordFile alice
New password:
Re-type new password:
Adding password for user alice
[root@fedora nehalparsekar]# htpasswd -m /etc/squid/passwordFile bob
New password:
Re-type new password:
Adding password for user bob
[root@fedora nehalparsekar]# htpasswd -c -m /etc/squid/passwordFile darth
New password:
Re-type new password:
Adding password for user darth
[root@fedora nehalparsekar]#
```

8. Allow access to all websites only after user authentication.

auth_param basic program /usr/lib64/squid/basic_ncsa_auth /etc/squid/passwordFile (First Line)

acl authusers proxy_auth REQUIRED

http_access allow authusers

http_access deny all

9. Allow access to Amazon and Flipkart only after user authentication. Allow free access to other sites.

acl blacklist dstdomain www.amazon.com

acl blacklist dstdomain www.flipkart.com

acl authusers proxy_auth REQUIRED

http_access allow blacklist authusers

http_access allow all

10. Allow Access to Amazon and Flipkart without authentication. Other sites need user to be authenticated.

acl blacklist dstdomain www.amazon.com

acl blacklist dstdomain www.flipkart.com

acl authusers proxy_auth REQUIRED

http_access allow blacklist

http_access allow !blacklist authusers

11. Allow Alice to access only Amazon and Flipkart. Allow Bob to access only YouTube and Twitter. No access to DARTH. No access without user authentication.

acl shopSites dstdomain www.amazon.com www.flipkart.com

acl socialSites dstdomain www.youtube.com www.twitter.com

acl bob proxy_auth bob

acl alice proxy_auth alice

acl dARTH proxy_auth dARTH

http_access allow alice shopSites

http_access deny alice !shopSites

http_access allow bob socialSites

http_access deny bob !socialSites

http_access deny all

12. Allow Alice access to Amazon and Flipkart only between 1 to 2pm, rest all the time. Allow Bob access to YouTube and Twitter only between 5 to 6 pm., rest all the time. Allow DARTH to access the four websites all the time and nothing else.

acl shopSites dstdomain www.amazon.com www.flipkart.com

acl socialSites dstdomain www.youtube.com www.twitter.com

acl aliceTime time 13:00-14:00

acl bobTime time 17:00-18:00

acl bob proxy_auth bob

acl alice proxy_auth alice

acl dARTH proxy_auth dARTH

http_access allow alice shopSites aliceTime

http_access allow alice !shopSites

http_access allow bob socialSites bobTime
http_access allow bob !socialSites
http_access allow darth socialSites
http_access allow darth shopSites
http_access deny darth !socialSites
http_access deny darth !shopSites
http_access deny all

13. Same as above. Allow DARTH to access all websites at all times.

acl shopSites dstdomain www.amazon.com www.flipkart.com
acl socialSites dstdomain www.youtube.com www.twitter.com

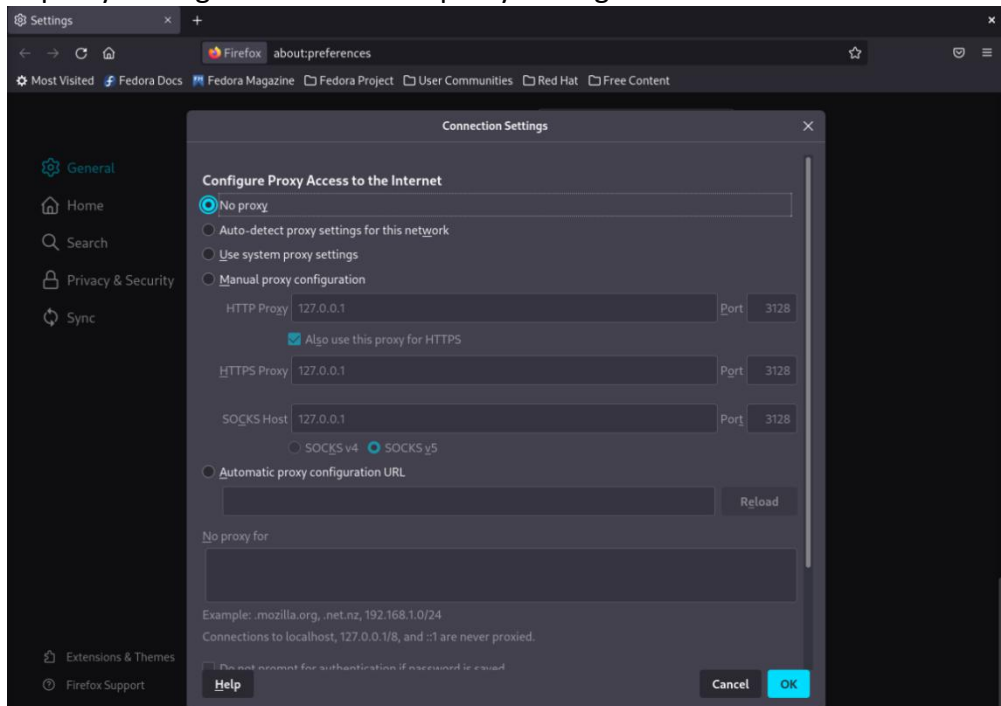
acl aliceTime time 13:00-14:00
acl bobTime time 17:00-18:00

acl bob proxy_auth bob
acl alice proxy_auth alice
acl darth proxy_auth darth

http_access allow alice shopSites aliceTime
http_access allow alice !shopSites
http_access allow bob socialSites bobTime
http_access allow bob !socialSites
http_access allow darth socialSites
http_access allow darth all
http_access deny all

SQUID (Transparent)

1. Change browser proxy setting – remove SQUID proxy settings.



2. Make changes to SQUID configuration file to enable transparent proxy.

http_port 3129 intercept

3. Restart proxy server.

systemctl restart squid.service

4. Add Iptables rules to route port 80 and port 443 traffic through SQUID.

iptables -t nat -A OUTPUT -p tcp -m tcp --dport 80 -m owner ! --gid-owner 23 -j REDIRECT --to-port 3129

iptables -t nat -A OUTPUT -p tcp -m tcp --dport 443 -m owner ! --gid-owner 23 -j REDIRECT --to-port 3129

```
[root@fedora nehalparsekar]# iptables -t nat -A OUTPUT -p tcp -m tcp --dport 443 -m owner ! --gid-owner 23 -j REDIRECT --to-port 3129
[root@fedora nehalparsekar]# iptables -t nat -A OUTPUT -p tcp -m tcp --dport 80 -m owner ! --gid-owner 23 -j REDIRECT --to-port 3129
[root@fedora nehalparsekar]# iptables -t nat -L OUTPUT
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:https ! owner GID match squid redir ports 3129
REDIRECT  tcp  --  anywhere              anywhere               tcp dpt:http ! owner GID match squid redir ports 3129
[root@fedora nehalparsekar]#
```

List of assignments to complete –Transparent Proxy mode.

1. Block Amazon and Flipkart.

acl blacklist dstdomain www.amazon.com

acl blacklist dstdomain www.flipkart.com

http_access deny blacklist

http_access allow all

2. Block all websites except Amazon and Flipkart.

acl blacklist dstdomain www.amazon.com

acl blacklist dstdomain www.flipkart.com

http_access allow blacklist

http_access block all

3. Block all websites between 9 am to 5 pm. (Since the lab is scheduled between 2 to 5 pm , all websites should be blocked).

acl mcaTime time 9:00-17:00

http_access deny mcaTime

http_access allow all

4. Block access to Amazon and Flipkart between 2 to 5 pm. Allow all other sites.

acl blacklist dstdomain www.amazon.com

acl blacklist dstdomain www.flipkart.com

acl blockShopTiming time 9:00-17:00

http_access deny blockShopTiming blacklist

http_access allow all